Technical Cybersecurity

Sabotage

Sabotage

More and more common

- Stuxnet
- BlackEnergy

High value targets hard to access

- Still use typical windows malware to get access to industrial control command & control channels
- Can be hard to trigger events

Stuxnet

ATTACKED URANIUM ENRICHMENT FACILITIES

- Spun the centrifuges too fast
- camouflaged real data (false data injection attack)
- Intermittent

BlackEnergy

Attacked Ukrainian power distribution

- Piggybacked on black market DDOS tool
- Extra code, extra payloads
- Active recon inside infrastructure
- Stole credentials, destroyed hardware

CrashOverride

TIED TO BLACKENERGY, FOUND IN UKRAINE

- Implant used in tandem with BlackEnergy
- Initial infection vector unknown
- Submits C&C data using international industrial control protocols
- Extensible, able to act with little control

Hatman

ATTACKED SAFETY SYSTEMS IN SAUDI ARABIA

- Windows component injects code into safety system
- Safety system receives commands via specially-crafted packets
- Written in python with specific PowerPC binaries injected into the controllers
- Second malware **ever** to manipulate actual ICS code (Stuxnet was the first)

Let’s talk about attack analysis next.